IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Dunstan et al.	Art Unit :	2132
Serial No.:	10/034,131	Examiner :	Samson B. Lemma
Filed:	December 28, 2001	Conf. No.:	1605

Title : SECURE DELIVERY OF ENCRYPTED DIGITAL CONTENT

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Applicant herewith files this brief on appeal under 37 CFR 41.37, thereby perfecting the notice of appeal which was originally filed on October 20, 2006.

The sections required by 37 CFR 41.37 follow.

(1) Real Party in Interest

This application is assigned of record to Intel Corporation who is hence the real party in interest.

(2) Related Appeals and Interferences

There are no known related appeals or interferences.

(3) Status of Claims

Claims 1-30 are pending, with claims 1, 14, 24, 27 and 29 being independent. Claims 1-30 stand rejected, and all of these claims are appealed herein.

(4) Status of Amendments

No claim amendments have been filed after final rejection.

(5) Summary of Claimed Subject Matter

The presently claimed subject matter is generally directed to systems and techniques relating to secure delivery of encrypted digital content. The claimed subject matter can isolate a decryption scheme within a decoder core, and thus the content decoder may be made independent of the encryption/decryption scheme to be used. This enables modification of content protection techniques that are to be used with an already publicly distributed content decoder.

Independent claim 1 defines a method comprising: transmitting a decoder core to be used with a predefined content decoder (*see, e.g.*, Specification at ¶s 20, 36 and 58, and reference numeral 350 in FIG. 3), the decoder core comprising instructions for causing the predefined content decoder to decrypt an encrypted version of digital content (*see, e.g.*,

Specification at ¶s 18-22 and 31-38, and reference numerals 225, 240 and 245 in FIG. 2).

Dependent claim 8 further specifies that the decoder core further comprises obfuscated software (*see, e.g.*, Specification at ¶s 37-39 and 52-56, reference numeral 225 in FIG. 2, and reference numerals 340 and 345 in FIG. 3). Dependent claim 9 further specifies that the obfuscated software comprises content-specific obfuscated software (*see, e.g.*, Specification at ¶s 20 and 37, reference numeral 225 in FIG. 2, and reference numerals 340 and 345 in FIG. 3).

Independent claim 14 defines a method comprising: receiving a decoder core comprising instructions for decrypting encrypted digital content (*see, e.g.*, Specification at ¶s 18-22, 31-38, 58 and 61, reference numeral 225 in FIG. 2, and reference numeral 405 in FIG. 4); and using the decoder core with a previously acquired content decoder to access the encrypted digital content (*see, e.g.*, Specification at ¶s 31-38 and 64, reference numerals 200, 220, 225, 240 and 245 in FIG. 2, and reference numeral 430 in FIG. 4).

Dependent claim 22 further specifies that the decoder core further comprises obfuscated software (*see, e.g.*, Specification at ¶s 37-39 and 52-56, reference numeral 225 in FIG. 2, and reference numerals 340 and 345 in FIG. 3). Dependent claim 23

further specifies that the obfuscated software comprises software that has been obfuscated with respect to the digital content (*see, e.g.*, Specification at ¶s 20 and 37, reference numeral 225 in FIG. 2, and reference numerals 340 and 345 in FIG. 3).

Independent claim 24 defines a machine-readable medium embodying information indicative of instructions (*see, e.g.*, Specification at ¶s 68 and 70, and reference numerals 506 and 508 in FIG. 5) for causing one or more machines to perform operations comprising: defining an interface between a presentation portion and a decryption portion of a digital content player (*see, e.g.*, Specification at ¶s 18 and 31-33, reference numerals 200, 205, 220 and 225 in FIG. 2); identifying a decoder core that uses the interface to effect the decryption portion of the digital content player (*see, e.g.*, Specification at ¶s 18-22 and 31-38, and reference numeral 225 in FIG. 2); and using the decoder core with the digital content player to access encrypted digital content (*see, e.g.*, Specification at ¶s 31-33, and reference numerals 200, 225, 240 and 245 in FIG. 2).

Independent claim 27 defines a content decoder comprising: a module defining an interface between the content decoder (*see, e.g.*, Specification at ¶s 18 and 31-33, and reference numerals 200 and 220 in FIG. 2) and a mutable decoder core comprising

instructions for causing the content decoder to decrypt encrypted media (*see, e.g.*, Specification at ¶s 18-22 and 31-38, and reference numerals 225, 240 and 245 in FIG. 2).

Independent claim 29 defines a system for facilitating secure delivery of digital content, the system comprising: means for transmitting in response to a request (*see, e.g.*, Specification at ¶s 23-30 and 47-60, reference numerals 105-120 in FIG. 1, and reference numerals 300-350 in FIG. 3), software plug-in means for decrypting digital content (*see, e.g.*, Specification at ¶s 18-22 and 31-38, and reference numeral 225 in FIG. 2); and means for receiving the software plug-in means and for presenting the digital content using the software plug-in means (*see, e.g.*, Specification at ¶s 18-22 and 31-38, reference numerals 130-140 in FIG. 1, reference numerals 200, 220 and 250 in FIG. 2, reference numerals 400-430 in FIG. 4, and reference numeral 500 in FIG. 5).

(6) Grounds of Rejection to be Reviewed on Appeal

I. Claims 1-30 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hurtado et al. (U.S. Patent 6,611,812) in view of Thompson et al. (U.S. Patent 5,406,627).

(7) Argument

A *prima facie* case of obviousness has not been established because there is no motivation to combine the references as suggested, and the proposed combination does not teach or suggest all the features of the claims. Hurtado describes a secure electronic content distribution system in which an end user system receives from a clearing house a secure container. This secure container contains a decrypting key for decrypting at least part of previously encrypted content, where this secure container has been encrypted using an encrypting key of the end user system. The end user system can then decrypt the secure container (using the encrypting key of the end user system) to access the decrypting key for decrypting at least part of the encrypted content. (*See* Hurtado at Abstract.)

In contrast, Thompson describes an audiovisual subscription system that includes means for aperiodically inverting the lines of a transmitted video signal on a frame-by-frame basis and for decrypting encrypted PCM (pulse-code-modulated) audio information which is transmitted along with the aperiodically inverted video information. (*See* Thompson at Abstract.) One skilled in the art would not be motivated to combined Thompson with Hurtado because they are directed to very different subject matter. It is noted that Thompson and Hurtado do not share a

common subject matter classification, and the motivation identified by the Office misstates the cited portion of Thompson as relating to data encryption, when in fact, it relates to data scrambling. (*See* Final Office Action mailed 07/20/2006 at pp. 3-4, and Thompson at col. 2, lines 43-47.)

Moreover, Hurtado actually teaches away from the proposed combination. Hurtado describes sending the data decryption keys to the end-user device as an added security of a secure electronic content distribution system. (*See e.g.*, Hurtado at Abstract, col. 10, lines 1-27, col. 17, line 51 to col. 18, line 62, and FIGs. 2-3) In contrast, Thompson describes having the data decryption keys be resident on the end-user device, and an appropriate decryption key is selected for a signal. (*See* Thompson at col. 9, lines 51-57; and col. 42, line 53 to col. 43, line 15.) Thus, Hurtado teaches away from the proposed combination with Thompson, and there is no motivation to combine the references as suggested.

In addition, even if Hurtado and Thompson could be combined as suggested, which is not conceded, the resulting combination would not teach or suggest all the features of the claims. Independent claim 1 recites, "transmitting a decoder core to be used with a predefined content decoder, the decoder core comprising instructions for causing the predefined content

decoder to decrypt an encrypted version of digital content." (Emphasis added.) The Office acknowledges that Hurtado does not describe a decoder core comprising instructions for causing the predefined content decoder to decrypt an encrypted version of digital content, and relies on Thompson for this feature of claim 1. However, the cited portion of Thompson makes clear that Thompson's instructions merely identify a decryption key (already present at the receiving device) to use with an already defined digital data decryption circuit. (*See* Thompson at col. 42, line 53 to col. 43, line 15.) These "instructions" of Thompson cannot be considered a decoder core as presently claimed.

The present application clearly describes the terms "content decoder" and "decoder core":

> A content decoder (e.g., a media player device such as a Tivo or a Replay device, media player software, or a component of these) can be logically divided into a replaceable decoder core and remaining portions. The decoder core implements a selected decryption scheme for decrypting encrypted content, and the remaining portions provide an interface between the decoder core and content presentation systems/devices. The decoder core may be changed as desired to implement a newly selected decryption scheme and/or to

> change the nature of the decoder core (e.g., a new software obfuscation, a new time-stamp).

(*See* the present application at ¶ 18; emphasis added.) As further detailed in the example encrypted digital content delivery and decoding system shown in Fig. 2:

> The content decoder 200 includes an interface 220 that defines how a received decoder core 225 is to be integrated with the content decoder 200. […] [T]he content decoder 200 receives a mutable software module. […] The interface 220 is a predefined interface that provides the hooks (e.g., procedure calls) with which the content decoder 200 runs the decoder core 225. In one implementation, the decoder core 225 is a software plug-in for the content decoder 200.

(*See* the present application at ¶s 31-33; emphasis added.)

The claimed subject matter can isolate the decryption scheme within the decoder core, and thus the content decoder may be made independent of the encryption/decryption scheme to be used. This enables modification of content protection techniques that are to be used with an already publicly distributed content decoder. (*See* the present application at ¶s 19-20.)

In contrast, Thompson describes a receiving device that already has the decryption components used to decrypt encrypted

digital content using a selected resident key. (*See* Thompson at FIGS. 2A" and 4B', reference symbols 134a, 134b, 465a, 465b, 466 and corresponding description.) The "instructions" in the cited portion of Thompson are not part of a decoder core and are not for causing a predefined content decoder to decrypt an encrypted version of digital content, because these instructions of Thompson simply inform the microprocessor which resident decryption key to use with a defined data decryption circuit. (*See* Thompson at col. 42, line 53 to col. 43, line 15.) For all of the above reasons, a *prima facie* case of obviousness has not been established for independent claim 1.

Independent claim 14 recites, "receiving a decoder core comprising instructions for decrypting encrypted digital content; and using the decoder core with a previously acquired content decoder to access the encrypted digital content." (Emphasis added.) For at least the reasons discussed above, Hurtado and Thompson are not properly combinable to realize the subject matter of claim 14, and neither Hurtado nor Thompson teach or suggest (alone or in combination) receiving a decoder core comprising instructions for decrypting encrypted digital content, and using the decoder core with a previously acquired content decoder to access the encrypted digital content. Thus,

a *prima facie* case of obviousness has not been established for independent claim 14.

In addition, independent claim 24 recites, "defining an interface between a presentation portion and a decryption portion of a digital content player; identifying a decoder core that uses the interface to effect the decryption portion of the digital content player; and using the decoder core with the digital content player to access encrypted digital content." (Emphasis added.) Independent claim 27 recites, "a module defining an interface between the content decoder and a mutable decoder core comprising instructions for causing the content decoder to decrypt encrypted media." (Emphasis added.) Independent claim 29 recites, "means for transmitting in response to a request, software plug-in means for decrypting digital content; and means for receiving the software plug-in means and for presenting the digital content using the software plug-in means." (Emphasis added.)

The Office has not addressed the language of claims 24, 27 and 29. Thus, a *prima facie* case of obviousness has not been established for these claims for at least this reason. Furthermore, for reasons similar to those discussed above, Hurtado and Thompson are not properly combinable to realize the subject matter of claims 24, 27 and 29, and neither Hurtado nor

Thompson teach or suggest (alone or in combination) defining an interface between a presentation portion and a decryption portion of a digital content player and identifying a decoder core that uses the interface to effect the decryption portion of the digital content player, a module defining an interface between the content decoder and a mutable decoder core, or software plug-in means for decrypting digital content. Thus, a *prima facie* case of obviousness has not been established for any of independent claims 24, 27 and 29.

A *prima facie* case of obviousness has not been established for any of dependent claims 2-13, 15-23, 25-26, 28 and 30 for at least the above reasons. In addition, claims 8-9 and 22-23 include various limitations related to obfuscated software included in the decoder core. The Office has not addressed these limitations, but rather rejects these claims without even discussing how the language of these claims is considered to read on the cited art. Thus, a *prima facie* case of obviousness has not been established for any of claims 8-9 and 22-23 for at least this additional reason.

Moreover, Hurtado is clearly directed to a system for delivering decryption keys, not decryption software. Hurtado remains agnostic regarding the specific encryption/decryption algorithms to be used in the system. (*See* Hurtado at col. 15,

line 29 to col. 16, line 48.) Furthermore, Hurtado provides no description whatsoever of software obfuscation, which can be used to make decryption software difficult to reverse engineer. These arguments were presented to the Office multiple times, and the Office has not responded to these arguments in any of the Office Actions.

For all of the above reasons, it is respectfully requested that Ground of Rejection I be overturned.

Please apply the brief fee in the amount of $500, the two month extension of time fee in the amount of $450, and any other necessary charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: Feb. 20, 2007

for Scott C. Harris
Reg. No. 32,030
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. **20985**
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

WILLIAM E. HUNTER
REG. NO 47,671

10701040.doc

Appendix of Claims

1. A method comprising:

transmitting a decoder core to be used with a predefined content decoder, the decoder core comprising instructions for causing the predefined content decoder to decrypt an encrypted version of digital content.

2. The method of claim 1, further comprising receiving a request to access digital content, wherein the transmitting comprises transmitting in response to the request.

3. The method of claim 2, further comprising generating the decoder core in response to the request.

4. The method of claim 3, wherein the decoder core further comprises information corresponding to the request.

5. The method of claim 4, wherein the information comprises a serial number for a session.

6. The method of claim 4, wherein the information comprises timing information.

7. The method of claim 1, wherein the decoder core further comprises a decryption key.

8. The method of claim 1, wherein the decoder core further comprises obfuscated software.

9. The method of claim 8, wherein the obfuscated software comprises content-specific obfuscated software.

10. The method of claim 9, wherein the content-specific obfuscated software corresponds to a content-specific encryption algorithm, the method further comprising:

encrypting the requested digital content using the content-specific encryption algorithm; and

delivering the encrypted digital content.

11. The method of claim 9, wherein the content-specific obfuscated software includes hashed portions of the digital content.

12. The method of claim 1, wherein the predefined content decoder comprises a previously delivered media player.

13. The method of claim 12, wherein the previously delivered media player comprises a satellite transmission receiving device, and wherein the transmitting a decoder core comprises transmitting the decoder core along with the encrypted version of the digital content from a satellite.

14. A method comprising:

receiving a decoder core comprising instructions for decrypting encrypted digital content; and

using the decoder core with a previously acquired content decoder to access the encrypted digital content.

15. The method of claim 14, wherein receiving a decoder core comprises receiving the encrypted digital content and the decoder core together.

16. The method of claim 15, wherein receiving the encrypted digital content and the decoder core together comprises receiving the encrypted digital content and the decoder core over a unidirectional network.

17. The method of claim 14, further comprising receiving the encrypted digital content separate from the decoder core.

18. The method of claim 17, wherein receiving the encrypted digital content comprises receiving the encrypted digital content on an optical disc, and the previously acquired content decoder comprises an optical disc playing device.

19. The method of claim 14, further comprising re-encrypting the digital content using an intra-home content protection scheme.

20. The method of claim 14, wherein receiving a decoder core comprises receiving the decoder core over a network in response to a request for access to the digital content, and wherein the decoder core further comprises information corresponding to the request.

21. The method of claim 20, wherein the information comprises a serial number and timing information, the method further comprising:

requesting a signed time check from a server;

comparing the signed time check with the timing information; and

preventing access to the encrypted digital content if the signed time check does not match the timing information within a

predetermined time difference.

22. The method of claim 14, wherein the decoder core further comprises obfuscated software.

23. The method of claim 22, wherein the obfuscated software comprises software that has been obfuscated with respect to the digital content.

24. A machine-readable medium embodying information indicative of instructions for causing one or more machines to perform operations comprising:

defining an interface between a presentation portion and a decryption portion of a digital content player;

identifying a decoder core that uses the interface to effect the decryption portion of the digital content player; and

using the decoder core with the digital content player to access encrypted digital content.

25. The machine-readable medium of claim 24, wherein defining an interface comprises establishing a public interface for a procedure in a class.

26. The machine-readable medium of claim 24, wherein the interface comprise a dynamic interface in which a portion of the interface is definable by the identified decoder core.

27. A content decoder comprising:

a module defining an interface between the content decoder and a mutable decoder core comprising instructions for causing the content decoder to decrypt encrypted media.

28. The content decoder of claim 27, wherein the interface comprises input and output format information for a decryption procedure to be defined by the mutable decoder core.

29. A system for facilitating secure delivery of digital content, the system comprising:

means for transmitting in response to a request, software plug-in means for decrypting digital content; and

means for receiving the software plug-in means and for presenting the digital content using the software plug-in means.

30. The system of claim 29, further comprising means for generating the software plug-in means in response to the request.

Evidence Appendix

None.

Related Proceedings Appendix

None.